# AFFIDAVIT OF MATTHEW K. O'NEILL

I, Matthew K. O'Neill, being first duly sworn, hereby depose and state as follows:

## I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS") and have been so employed since 1998. I received formal training at the Federal Law Enforcement Training Center ("FLETC") in Glynco, Georgia, and the United States Secret Service Academy in Beltsville, Maryland. I am currently assigned to the United States Secret Service, Manchester Resident Office. My current assignment includes investigating violations of Title 18, United States Code, Sections 1028, 1029, 1030, 1341, 1343, 1344 and 1956 on the internet. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit various crimes.

2. As set forth herein, the USSS is currently investigating individuals who are hacking into the computer terminals of retailers, and in turn stealing their login credentials to a credit report database owned by Experian. The bad actors then query individuals to obtain their full credit report, which includes personal information such as name, date of birth, social security number, address, and bank account information, all in violation of 18 U.S.C. §§ 1030 (computer fraud and abuse), 1028 (identity fraud), and 1343 (wire fraud). A number of the individuals who had their credit reports queried are residents of New Hampshire.

3. The investigation to date has identified more than 55 compromised Experian credentials that were assigned to businesses and over 12,000 credit reports have been queried. Some of these other compromised merchants include Stamford Postal Credit Union, Chief Financial Credit Union, Palm Desert National Bank, Saratoga Homes, Morongo Band of Mission Indians Casino Resort and Spa, Verizon Wireless, Sallie Mae, El Paso Police Academy, and the Paterson Police Federal Credit Union.

4. As set forth below, using **ssndob.sll@gmail.com, hieupc@gmail.com, usafree12@gmail.com, iloveuv3@gmail.com, kinkonnens@gmail.com, alexdans07@googlemail.com, gregory.payne08@gmail.com, and cafenaumk@gmail.com**, the targets have discussed and/or received access to stolen personal identifying information (PII).

5. I am submitting this affidavit in support of an Application for a Search Warrant to search records and other information (including the contents of communications) associated with certain accounts, specifically: **ssndob.sll@gmail.com, hieupc@gmail.com, usafree12@gmail.com, iloveuv3@gmail.com, kinkonnens@gmail.com, alexdans07@googlemail.com, gregory.payne08@gmail.com, and cafenaumk@gmail.com** , that is stored at premises owned, maintained, controlled, or operated by Google Inc., an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A.

6. Based on my training and experience, and the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030, 1028

& 1343 have been committed by unknown targets/suspects. There is also probable cause to believe that records and other information associated with e-mail accounts **ssndob.sll@gmail.com, hieupc@gmail.com, usafree12@gmail.com, iloveuv3@gmail.com, kinkonnens@gmail.com, alexdans07@googlemail.com, gregory.payne08@gmail.com, and cafenaumk@gmail.com** as described in Attachment A, contain evidence, fruits, and/or instrumentalities of various violations of Title 18, United States Code, Sections 1030, 1028 & 1343, as detailed and specified herein below. Accordingly, there is probable cause to search the information described in Attachment A for evidence, fruits, and/or instrumentalities of these crimes, as described in Attachment B. This affidavit is made in support of an Application for a Search Warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to compel Google, a provider of electronic communication and remote computing services, to provide certain items as set forth in Attachment B, Part I, hereto, and for the government to search and to seize certain items as set forth in Attachment B, Part II, hereto.

7. The facts set forth in this affidavit are based upon my personal observations, my review of documents and computer records, my training and experience, and information obtained from other agents and witnesses, including from other law enforcement agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge of the investigation into this matter.

## II. PROBABLE CAUSE

8. Your affiant believes that there is probable cause to believe that evidence, instrumentalities, and/or fruits of criminal activity will be found in a search of computer servers hosted at Google, for the following reasons. In or about November 2010, the USSS was notified by Experian that they were experiencing losses due to unauthorized credit report queries on customers' accounts. The accounts that had apparently been compromised had been assigned to various merchants such as credit unions, banks, and other merchants that perform credit checks. Over 50 merchants had their Experian login credentials stolen and over 12,000 credit reports have been queried by the bad actors.

9. Further investigation, including interviews with representatives of financial institutions, third party forensic examiners, and individual victims, revealed that the Experian login credentials were stolen after the merchant was compromised via malware such as ZeuS. In fact, ZeuS malware varients were identified in the majority of the compromises in which the suspect malware was located.

10. Further investigation, including interviews with representatives from Experian's corporate headquarters, has identified at least eight New Hampshire residents who had their credit reports queried without authorization using one of the aforementioned compromised login credentials.

11. Throughout this investigation, I have communicated regularly with Investigator Scott Moore, Experian, a company located in California that is one of the three main credit bureaus in the United States. I have communicated with other Experian information technology (IT) and investigative representatives as well. Experian clients have engaged third-party

computer forensic examination firms, which have conducted various forensic examinations on the compromised terminals. I have reviewed reports summarizing the findings of those examinations.

12. As a result of my discussions with Moore and review of written materials provided by Moore and others at Experian relating to his investigative activities, I have learned that various types of malicious software called "keystroke loggers" ("KSL") had been installed on Experian's clients computers, that the programs were storing login credentials, and that the programs were uploading the data from the victim merchant's terminals to another location to be used to query credit reports.

13. During the course of the investigation it has been learned that a website identified as findget.me offers to sell personal information in a searchable format. The website states that anyone can purchase someone's identifiers; such as first name/last name/middle name/email address/email password/address/phone/DOB/Drivers License #/Bank Name/Bank account number/Bank Routing Number/Company name/Current years on job/mother's maiden name. Open source searches advise that this site is hosted by Westhost, 164 North Gateway Drive, Providence, UT 84332. The contact email address for this site is rr2518@gmail.com.

14. On February 3, 2012, Google responded to a Federal Search Warrant issued in the District of New Hampshire on January 31, 2012, for rr2518@gmail.com . Analysis of the contents of this email account revealed that rr2518@gmail.com sent personal identifying information to a number of other Google accounts.

15. On November 18, 2011, ssndob.sll@gmail.com sent rr2518@gmail.com an email that advises, "Hi! How are you? the old admin of superget.info told me that he sold his site to you, and now you are the new admin. He also told me that everything is the same as before for me reseller site extrascore.info. so let me know if you have something notes me. I wish we will have the best cooperation from now. Thanks. Have a good day!" On the same date, rr2518@gmail.com responds to ssndob.sll@gmail.com, "Hi mate! It's still normal for everything. $4600 for 4000 credits and $500 for server fee. Please pay to our LR: U8109093 (Traci Donell) Thanks u." On November 22, 2011, rr2518@gmail.com received an email from ssndob.sll@gmail.com which advises that he sent $4,600 to rr2518@gmail.com's Liberty Reserve account. On November 26, 2011, ssndob.sll@gmail.com sent an email to rr2518@gmail that states "I wrote to hieupc, I think your method that deducts credit even if they don't find an thing is not good mthod. Please think twice before aply it. you can change plan or do auto delete history, just don't do this way." On December 1, 2011, ssndob.sll@gmail.com sent rr2518@gmail.com an email which states "ok I see, no problem. I got $7500 now. Need to have $2500 more. Will you need that $10,000 tonight (asian time) or can I pay tomorrow?" On December 2, 2011, ssndob.sll@gmail.com sent an email to rr2518@gmail.com that shows that he sent $10,000 to rr2518@gmail.com's Liberty Reserve account.

16. On November 19, 2011, rr2518@gmail.com forwarded hieupc@gmail.com an email from ssndob.sll@gmail.com. Open source searches show that hieupc@gmail.com is associated with Hieu Minh Ngo. The ssndob.sll@gmail.com email appears to be written in Vietnamese, based on a query from microsofttranslator.com. RR2518@gmail.com writes to hieupc@gmail.com, "I don't know what he wrote, can you help me?" On November 26, 2011, ssndob.sll@gmail.com sent an email to rr2518@gmail.com that states "I wrote to hieupc, I think your method that deducts credit even if they don't find an thing is not good mthod. Please think twice before aply it. you can change plan or do auto delete history, just don't do this way." A Federal Search Warrant was issued in the District of New Hampshire for findget.me. Analysis of the login data from findget.me revealed that a user named hieupc logged into this website, as an administrator, from multiple IP addresses over a prolonged period of time.

17. On November 19, 2011, rr2518@gmail.com sent an email to usafree12@gmail.com which states "hi, Now please pay credits or server fees to me. Please pay $500 for server this month. Our LR is: U8109093 (Traci Donell) Let me know when you need credits. Thanks". For every search a person conducts in the database on the target's website, a certain number of credits is deducted. For example, a preset number of credits is deducted for, by way of example each social security number, or each date of birth that are accessed. Customers purchase credits prior to searching the database on the target's website by sending money through the website's Liberty Reserve account, which is an electronic currency payment channel which is difficult for law enforcement to track.

18. On November 20, 2011, iloveuv3@gmail.com sent rr2518@gmail.com an email that states "I have 2500 credit in account chanvailon. Why I can't access to my account :( " RR2518@gmail.com responded to this email "u just have 1592 credits in ur account. don't lie to us. Your new pass: 123456. Thx u."

19. On November 20, 2011, kinkonnens@gmail.com sent rr2518@gmail.com an email with subject line "your base." The body of the email states "also, we interested to buy your base if it's possible." rr2518@gmail.com responds "$500,000 for this base." This email appears to suggest that kinkonnens@gmail.com is interested in purchasing findget.me's database of PII.

20. On December 6, 2011, alexdans07@googlemail.com sent rr2518@gmail.com an email that advises that he sent $5,000 to Liberty Reserve account U4875739 from batch 78385412. This sender appears to be from "BackStab admin," which is another reseller of findget.me's database of personal identifying information.

21. On December 19, 2011, gregory.payne08@gmail.com sent rr2518@gmail.com an email that advises that he sent $150 to rr2518@gmail.com's Liberty Reserve (LR) account U8109093 from LRU2263642 on the same date at 22:51. On the same date, rr2518@gmail.com sent gregory.payne08@gmail.com an email that contains approximately 520 individuals PII to include name, email address, email address password, address, phone number, DOB, SSN, bank account number, bank account routing number, bank name, employer, years of service.

22. On January 10, 2012, rr2518@gmail.com sent cafenaumk@gmail.com an email that contains approximately 270 individuals PII to include name, email address, email address password, address, phone number, DOB, SSN, bank account number, bank account routing number, bank name, employer, years of service.

17. Based on my review of the records and other evidence obtained to date in this investigation, I believe that there is probable cause to believe that the suspect e-mail accounts set forth below contain fruits, instrumentalities or evidence of the identity theft scheme.

## III. TECHNICAL BACKGROUND

21. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Google allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the e-mail accounts, **ssndob.sll@gmail.com, hieupc@gmail.com, usafree12@gmail.com, iloveuv3@gmail.com, kinkonnens@gmail.com, alexdans07@googlemail.com, gregory.payne08@gmail.com, and cafenaumk@gmail.com,** listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information.

22. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on a Google server indefinitely.

23. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google server, the e-mail can remain on a Google server indefinitely.

24. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

25. A Google subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Google.

26. Subscribers to Google might not store on their home computers copies of the e-mails stored in their Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

27. In general, e-mail providers like Google ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

28. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

29. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

30. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

## IV. RELEVANT FEDERAL OFFENSES

31. Based upon the information above, your affiant believes that there is probable cause to believe that on the computer systems owned, maintained, and operated by Google, as described above, there exists evidence, fruits, and/or instrumentalities of violations of Title 18 United States Code, Section 1028 – Identity Theft; Section 1030 – Computer Fraud and Abuse; and Section 1343 -Wire Fraud, allowing agents to seize records and other information (including content of communications) stored on servers being maintained by Google for the account and files associated with the e-mail accounts: **ssndob.sll@gmail.com, hieupc@gmail.com, usafree12@gmail.com, iloveuv3@gmail.com, kinkonnens@gmail.com, alexdans07@googlemail.com, gregory.payne08@gmail.com, and cafenaumk@gmail.com.**

## V. LEGAL AUTHORITY AND INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

32. If issued, I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the

warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) located at the premises described in Attachment A ("Place to Be Searched") and particularly described in Attachment B, Part I ("Information to Be Disclosed by Google"). Upon receipt of the information described in Part I of Attachment B, government-authorized persons will review that information to locate the items described in Part II of Attachment B ("Information to Be Seized by the Government").

33. The government may obtain internet and e-mail content and subscriber information from a third party by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A). Any court with jurisdiction over the offense under investigation may issue a § 2703 warrant, regardless of the location of the server where information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike Rule 41 search warrants, a § 2703 warrant does not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

34. If the government obtains a search warrant, there is no requirement that the third party give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), (c)(3).

## VI. CONCLUSION

35. Based on my training and experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that unknown targets have committed Computer Fraud and Abuse in violation of 18 U.S.C. § 1030, Identity Theft in violation of 18 U.S.C. § 1028, and Wire Fraud in violation of 18 U.S.C. § 1343. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that computer systems owned or operated by or in the control of Google, an e-mail service provider located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, contain evidence, fruits, and instrumentalities of the crimes identified above. Accordingly, a Search Warrant is requested.

36. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A).

Special Agent Matthew K. O'Neill
United States Secret Service

Subscribed and sworn to before me
This 9th day of May, 2012

Landya B. McCafferty
United States Magistrate Judge

# ATTACHMENT A

## Place to Be Searched

This warrant applies to information associated with the e-mail accounts **ssndob.sll@gmail.com, hieupc@gmail.com, usafree12@gmail.com, iloveuv3@gmail.com, kinkonnens@gmail.com, alexdans07@googlemail.com, gregory.payne08@gmail.com, and cafenaumk@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Ampitheatre Parkway, Mountain View, CA 94043.

# ATTACHMENT B

## Particular Things to be Seized

### I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails stored in the account(s), including copies of e-mails sent to and from the account(s), draft e-mails, the source and destination addresses associated with each e-mail; the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was created, the length of service, the types of service utilized, the IP address used to register the account(s), log-in IP addresses associated with session times and dates, account(s) status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account(s), including address books, contact and buddy lists, calendar data, pictures, and files;

d. All records pertaining to communications between Google, Inc. and any person regarding the account(s), including contacts with support services and records of actions taken.

### II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and/or instrumentalities of violations of computer fraud and abuse (18 U.S.C. §1030), identity fraud (18 U.S.C. §1028), and wire fraud (18 U.S.C. § 1343), including, for the account(s) or identifier(s) listed on Attachment A, information relating to the following matters:

1. Records and data relating to the personal identifying information to include: first name/last name/middle name/email address/email password/address/phone/DOB/Drivers License #/Bank Name/Bank account number/Bank Routing Number/Company name/Current years on job/mother's maiden name.

2. Records and data relating to Liberty Reserve, libertyreserve.com, which is findget.me's on accepted source for payment.

3. Records and data relating to communications with the URL findget.me.

4. Records and data relating to communications with any WestHost server.

5. Records and data relating to communications with other e-mail accounts or instant message accounts (including, but not limited to, Messenger accounts) regarding any of the above.

6. Records and data relating to who used, created, or communicated with the account(s) or identifier(s), including records about their identities and whereabouts.

7. Records and data relating to the use, or attempted use, of personal identifying information to make purchases or establish credit.